(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 April 2001 (12.04.2001)

PCT

(10) International Publication Number
WO 01/25060 A2

(51) International Patent Classification[7]: B60R 25/00

(21) International Application Number: PCT/US00/27098

(22) International Filing Date: 2 October 2000 (02.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/157,060 1 October 1999 (01.10.1999) US

(71) Applicant: SIEMENS AUTOMOTIVE CORPORATION [US/US]; 2400 Executive Hills Drive, Auburn Hills, MI 48326 (US).

(72) Inventor: DESAI, Tejas; 43521 Holmes Drive, Sterling Heights, MI 48314 (US).

(74) Agents: SLENZAK, Laura, M.; c/o KELLER, Elsa, Siemens Corporation, 186 Wood Avenue South, Iselin, NJ 08330 et al. (US).

(81) Designated State *(national)*: JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/25060 A2

(54) Title: RELAY ATTACK DETECTION OF A SECURE VEHICLE COMMAND COMMUNICATION

(57) Abstract: A passive remote entry system evaluates the delay between a challenge signal from security system and a response signal from the passive fob. If the delay exceeds a threshold identification fails and the access is denied. The fob utilizes the signal from the security system as a reference signal for transmitting its response signal. The security system generates a challenge signal with a changing frequency, which is compared to the frequency of the response signal. Any lag in the change of the frequency in the response signal compared to the change in the frequency of the challenge signal is indicative of the amount of delay between the challenge and response signal.

RELAY ATTACK DETECTION OF A SECURE VEHICLE COMMAND COMMUNICATION

BACKGROUND OF THE INVENTION

The present invention relates to a vehicle security system, and more particularly to a passive remote entry system that is resistant to relay attacks.

Remote control units such as key fobs for remotely controlling functions of vehicles are well known. Currently, the original equipment for many vehicles includes a wireless transmitter for arming/disarming the car alarm and/or locking or unlocking the car doors. Furthermore, other systems are available which control these and other functions, such as energizing the car starter to start the engine.

The user selects the desired function by pressing the associated button on the transmitter keypad, and the transmitter responds by transmitting the appropriate signal and/or code. However, this requires a user to have access to the transmitter and press the associated button. Passive systems have been developed which automatically activate a vehicle system when the key fob is within a predefined distance of the vehicle. Commonly, passive systems provide an encrypted challenge response two-way communication system to prevent unauthorized activation.

A relay attack scheme may allow an unauthorized attack to defeat the security. In such a two-way relay attack, a first attacker is located adjacent the vehicle while a second attacker follows the vehicle owner who has left the vicinity of the vehicle and is carrying the passive remote fob. The first attacker triggers the desired vehicle function such as unlock or start engine and receives the challenge signal from the vehicle. The first attacker captures the challenge signal with a scanner type device and transmits the challenge signal to the second attacker. The second attacker receives the challenge signal from the first attacker and retransmits the challenge signal to the vehicle owner. The passive remote fob carried by the owner receives the vehicle challenge and responds with a proper response signal. The response signal is captured by the second attacker who then relays the signal back to the first attacker. The first attacker receives the response signal from the first attacker and retransmits the response signal to the vehicle. The first attacker then has access to the desired vehicle function. This sort of attack will defeat most encryption systems as the proper response signal is obtained from the true owner.

Accordingly, it is desirable to provide a passive remote system which will defeat such a two-way relay attack.

SUMMARY OF THE INVENTION

The present invention provides a passive remote system which will defeat the two-way relay attack described above. Generally, the present invention defeats the two-way relay attack by determining the amount of delay between the challenge signal and the response signal. However, rather than simply measuring time of flight directly, the fob of the present invention utilizes the incoming wireless signal from the vehicle as its reference isolator, upon which the frequency of the transmitted signal from the fob is based. Generally, by changing the frequency transmitted from the vehicle security system, the vehicle security system cam determine how much delay there is between the change in the frequency of the challenge signal and the change in the frequency in the response signal from the fob. The vehicle security system accomplishes this by mixing its reference signal with a derivative of the signal received from the fob and evaluating the difference in frequency.

For example, the base signal in the vehicle security system is preferably a ramp oscillating signal, increasing in frequency. Because the fob utilizes the signal received from the vehicle security system as its reference signal, the signal from the fob is also increasing in frequency (although preferably at a much higher frequency). The vehicle security system then compares the signal received from the fob to its base signal (the ramp oscillator). The amount by which the frequency of the base ramp oscillator and the signal from the fob differ is representative of the delay from the time the signal is transmitted from the vehicle security system to the fob, through the circuitry in the fob, and back to the vehicle security system. If this air frequency exceeds a predetermined threshold, the delay is to great, identification fails and the access to the vehicle is denied.

Preferably, the fob transmits at a frequency several orders have made it to greater than that transmitted the vehicle. Thus, the ramp oscillator signal received by the fob must be stepped up several orders of magnitude before being transmitted by the fob and stepped down several orders of magnitude before being compared by the

vehicle security system. This introduces some minor delay, which can be accounted for. However, this introduces a much greater delay in the circuitry in the would be attackers.

BRIEF DESCRIPTION OF THE DRAWINGS

The various features and advantages of this invention will become apparent to those skilled in the art from the following detailed description of the currently preferred embodiment. The drawings that accompany the detailed description can be briefly described as follows:

Figure 1 is a high level schematic of the passive remote entry system of the present invention, as implemented in a vehicle.

Figure 2 is an example of a more detailed schematic for implementing the passive remote entry system of the present invention.

Figure 3 is a graph illustrating the challenge and response signal of the passive remote entry system.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention provides a passive remote entry system 10 for a vehicle 12, shown generally in Figure 1. The passive remote entry system 10 includes a vehicle security system 14 installed on vehicle 12 and controlling access to and the operation of the vehicle operation of the vehicle 12 in a known matter, including operation of door latches, door locks, and the ignition and/or operation of the vehicle engine. The pass remote entry system 10 further includes a passive key fob 16 that is portable relative to the vehicle 12 and carried by the user. As in known passive remote entry systems, the present invention generally utilizes a challenge/response method for implementing passive remote entry. Generally, the vehicle security system 14 generates a wireless challenge signal, such as in response to attempted operation of a door latch, vehicle motion, or the detection of a presence near the vehicle. The wireless challenge signal is received by the fob 16, which in turn responds with a wireless response signal. If the proper response signal is received by the vehicle security system 14, identification is successfull and access to the vehicle 12 is permitted. The vehicle security system 14

and fob 16 may use any of numerous known techniques, including encryption or rolling codes.

According to the present invention, to prevent relay attacks, the vehicle security system 14 evaluates the delay between the challenge signal that it transmitted and the response signal it received. This is accomplished by using the challenge signal from the vehicle security system as the reference oscillator for the response signal transmitted by the fob 16. By changing the frequency of the challenge signal and comparing the frequency of the challenge signal with the frequency of the response signal from the fob 16, the difference in frequency is representative of the delay between the challenge signal and the response signal.

Preferably, the passive remote entry system 10 of the present invention first utilizes a more typical challenge/response technique in which the vehicle security system 14 transmits an encrypted challenge signal, to which the fob 16 responds with an encrypted response signal, which is evaluated by the vehicle security system 14. If the proper response signal is received, then the passive remote entry system 10 subsequently proceeds with the evaluation of delay, in which the fob 16 then uses the challenge signal as a reference oscillator and the vehicle security system 14 compares the frequencies of the challenge signal and response signal.

Preferably, the challenge signals transmitted from the vehicle security system is low frequency, preferably less then one MHz, and preferably around 125 kHz. This reduces the range of the challenge signal to the area immediately adjacent the vehicle 12. The fob 16 preferably transmits the response signals at a frequency several orders of magnitude greater than that of the challenge signals. Preferably, the response signals are transmitted at a frequency greater than 100 MHz and more preferably at or around 315 MHz. Thus, for the fob 16 to use the challenge signal as a reference oscillator, the challenge signal is first stepped up several orders of magnitude. Similarly, before the vehicle security system 14 can compare the frequency of the response signal with the frequency of its reference oscillator, the frequency of the response signal must be stepped down several orders of magnitude. This introduces a slight delay from the circuitry in the fob 16 in vehicle security system 14, but several orders of magnitude

lower than the delay which would be introduced by the circuitry of the would-be relay attackers.

Sample circuits which could be utilized for the vehicle security system 14 and fob 16 of the present invention are shown schematically in Figure 2. The values shown in the schematic are for purposes for illustrating the preferred embodiment in which the challenge signal is transmitted at a 125 kHz and the response signal is transmitted at 315 MHz. Of course, other values and other circuits could be utilized. The vehicle security system 14 includes a micro controller 20 which implements the rolling codes or encrypted codes and controls operation of the vehicle security system 14. A coded challenge signal is first sent from micro controller 20 to switch 22 to send an amplitude shift keyed code via the antenna 24 based upon a reference oscillator 26, which may be a voltage controlled oscillator. Initially, the oscillator 26 is operating at a 125 kHz.

The 125 kHz signal is received by fob 16 on antenna 30 and amplified by buffers 32. The coded signal is then demodulated by detector 34 and sent to micro controller 36 which evaluates the code. The micro controller 36, using the same encryption or rolling code technique as the micro controller 20 in the vehicle security system 14, sends a proper coded response signal using amplitude shift keying on switch 38 which is connected to the oscillator 40 which is controlled by crystal 42. As controlled by the micro controller 36, a switch 43 connects the crystal-controlled oscillator 40 to the amplitude shift key switch 38. This high frequency signal from oscillator 40 is stepped down by frequency divider 44 prior to the amplitude shift keying by switch 38 and then transmitted via the antenna 46.

The 315 MHz amplitude shift key coded response signal transmitted from the antenna 46 on the fob 16 is received by the receiving antenna 50 on vehicle security system 14. A 9.509375 GHz crystal 52 controls oscillator 54 to provide an oscillating signal which is stepped down by frequency divider 56 to provide a 304.3 MHz signal which is mixed with the 315 MHz signal received from the fob 16 on antenna 15. Resulting 10.7 MHz signal 58 is buffered by buffers 60, and evaluated by micro controller 20. If the proper coded response signal is received by micro controller 20, then the micro controller 20 proceeds to an evaluation of the delay during a subsequent challenge and response signal, which may also use encryption or rolling codes.

The micro controller 20 then controls voltage control oscillator 26 to provide a ramp oscillating signal, preferably centered around 125 kHz. The signal is transmitted by antenna 24 and received by antenna 30 of the fob 16. Micro controller 36 controls switch 43 to utilize the incoming signal on antenna 30 as the reference oscillator (rather than oscillator 40 with crystal 42). This low frequency signal, centered around 125 kHz, is stepped up by frequency multiplier 70, stepped down by frequency divider 44 and amplitude shift key modulated by switch 38 and micro controller 36 and transmitted by antenna 46. The oscillating signal from voltage-controlled oscillator 26 is amplitude shift key modulated by switch 22 in micro controller 20 and transmitted by antenna 24. Because the fob 16 is now using the received challenge signal (centered around 125 kHz) as its reference oscillator, the response signal from the fob 16 (centered around 215 MHz) changes accordingly. This response signal is received by antenna 50 on the vehicle system 14 and mixed down to 125 kHz . This signal is then mixed with the signal from the voltage controlled oscillator 26 by mixer 76. The resulting signal is an error frequency 78, the frequency of which is equal to the difference between the frequency of voltage controlled oscillator 26 and that of the step down frequency of the response signal from the fob 16. This error frequency 78 is evaluated by micro controller 20 and/or additional hard-wired circuitry. If the error frequency 78 exceeds a predetermined threshold, then the delay between the challenge signal and response signal is determined to be to great and identification fails and access is denied to the vehicle 12.

For example, if there were zero delay in the circuitry of the vehicle security system 14 and the fob 16 and zero delay between the two circuits, the stepped down frequency of the response signal would match the frequency of the voltage control oscillator 26 and the error frequency 78 would be zero (or dc). However, because the frequency of the voltage controlled oscillator 26 is increasing, delay between the challenge signal and response signal results in the frequency of the voltage controlled oscillator 26 being higher than that of the stepped down response signal at mixer 78, and thus a higher error frequency 78.

This is illustrated in the graph of Figure 3. As can be seen in Figure 3, the frequency of the challenge signal increases over time (preferably, but not necessarily

linearly). The slope of the response signal from the fob 16 (shown stepped down to the 125 kHz range) is the same if that of the challenge signal, although shifted to the right by the amount of delay, shown as delta t. What the present invention measures, however, is the error frequency, which as can be seen, is directly representative of the delay, delta t. It is anticipated that delta t for a proper response signal from the fob 16 would be on the order of 100 ns. While the delta t for a relay attack signal would be on the order of several microseconds, and would thus result in a much higher error frequency (depending upon the slope of the challenge signal).

In accordance with the provisions of the patent statutes and jurisprudence, exemplary configurations described above are considered to represent a preferred embodiment of the invention. However, it should be noted that the invention can be practiced otherwise than as specifically illustrated and described without departing from its spirit or scope. Alphanumeric labels on method steps in the claims below are for convenience of reference by dependent claims, and do not signify a required order of performance of the method steps.

CLAIMS

1. A method for providing remote wireless identification including the steps of:

a) transmitting a wireless challenge signal;

b) receiving the challenge signal;

c) transmitting a wireless response signal in response to said step b);

d) receiving said response signal; and

e) evaluating a delay between said step a) and said step d).

2. The method of claim 1 further including the step of:

f) denying identification based upon said step e).

3. The method of claim 1 further including the steps of:

f) transmitting the wireless challenge signal at a challenge frequency in said step a);

g) using the challenge signal challenge frequency as a reference frequency for a response frequency, wherein the response frequency is based upon the challenge frequency; and

h) transmitting the wireless response signal in said step c) at the response frequency.

4. The method of claim 3 wherein the response frequency is a multiple of the challenge frequency.

5. The method of claim 4 further including the step of:

h) changing the challenge frequency and the response frequency over time.

6. The method of claim 5 further including the step of increasing the challenge frequency and response frequency over time.

7. The method of claim 6 wherein said step e) further includes the step of evaluating a difference between the challenge frequency and response frequency to determine the delay.

8. The method of claim 7 wherein the challenge frequency is a low frequency.

9. The method of claim 8 wherein the challenge frequency is less than 1 MHz.

10. The method of claim 8 wherein the response frequency is at least one thousand times the challenge frequency.

11. A method for providing remote wireless identification including the steps of:

a) transmitting a wireless challenge signal at a challenge frequency;

b) changing the challenge frequency of the challenge signal during said step a);

c) receiving the challenge signal;

d) determining a response frequency based upon the challenge frequency using the challenge frequency as a reference;

e) transmitting a wireless response signal at the response frequency in response to said step b).

12. The method of claim 11 wherein the response frequency is a multiple of the challenge frequency.

13. The method of claim 11 further including the step of:

i) changing the challenge frequency and the response frequency over time.

14. The method of claim 13 further including the step of increasing the challenge frequency and response frequency over time.

15. The method of claim 14 further including the step of evaluating a difference between the challenge frequency and response frequency to determine a delay.

16. The method of claim 15 further including the step of denying identification based upon the delay exceeding a threshold.

17. A security system comprising:

A first transmitter and first receiver in a security system, said first transmitter sending a challenge signal at a challenge frequency;

A second transmitter and second receiver on a fob, portable relative to the security system, said second transmitter sending a response signal in response to the challenge signal, said second transmitter sending said response signal at a response frequency based upon said challenge frequency, using said challenge frequency as a reference oscillator.

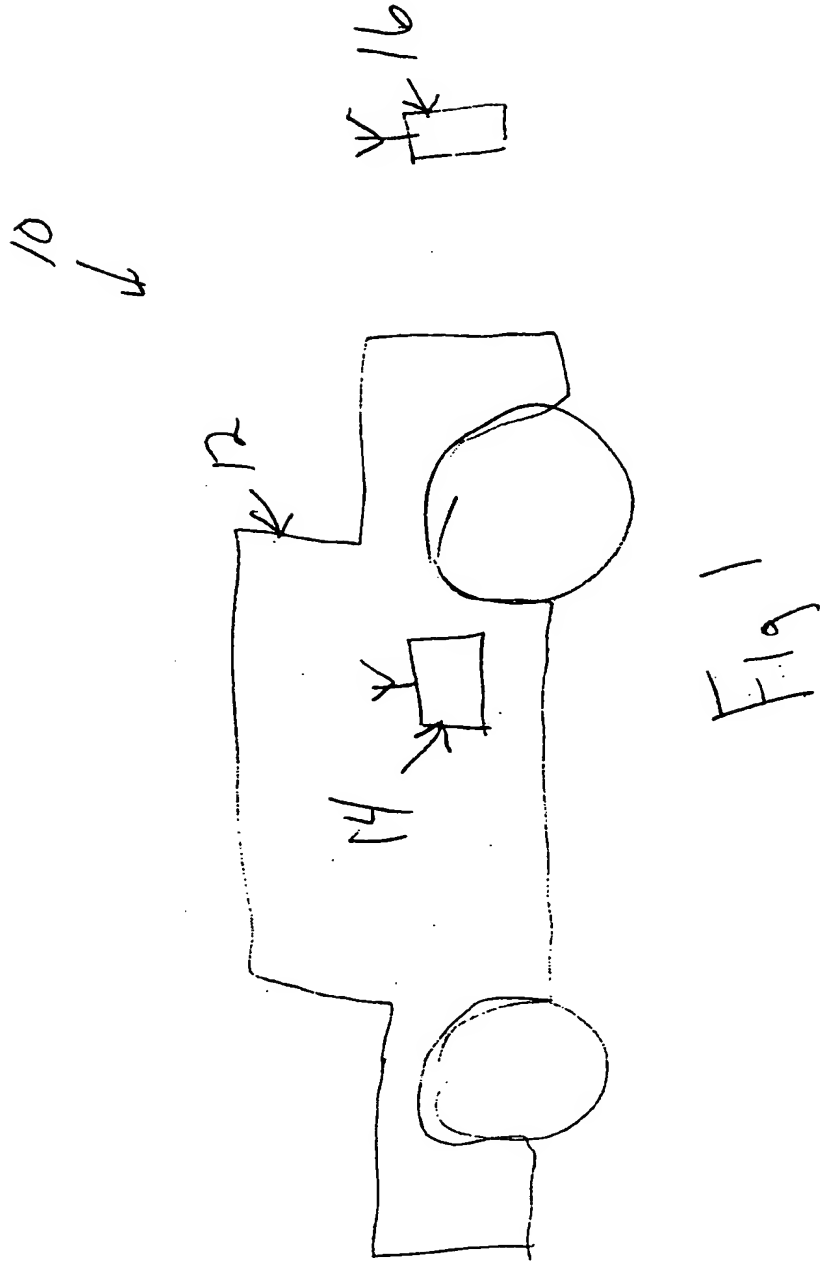

FIG. 1

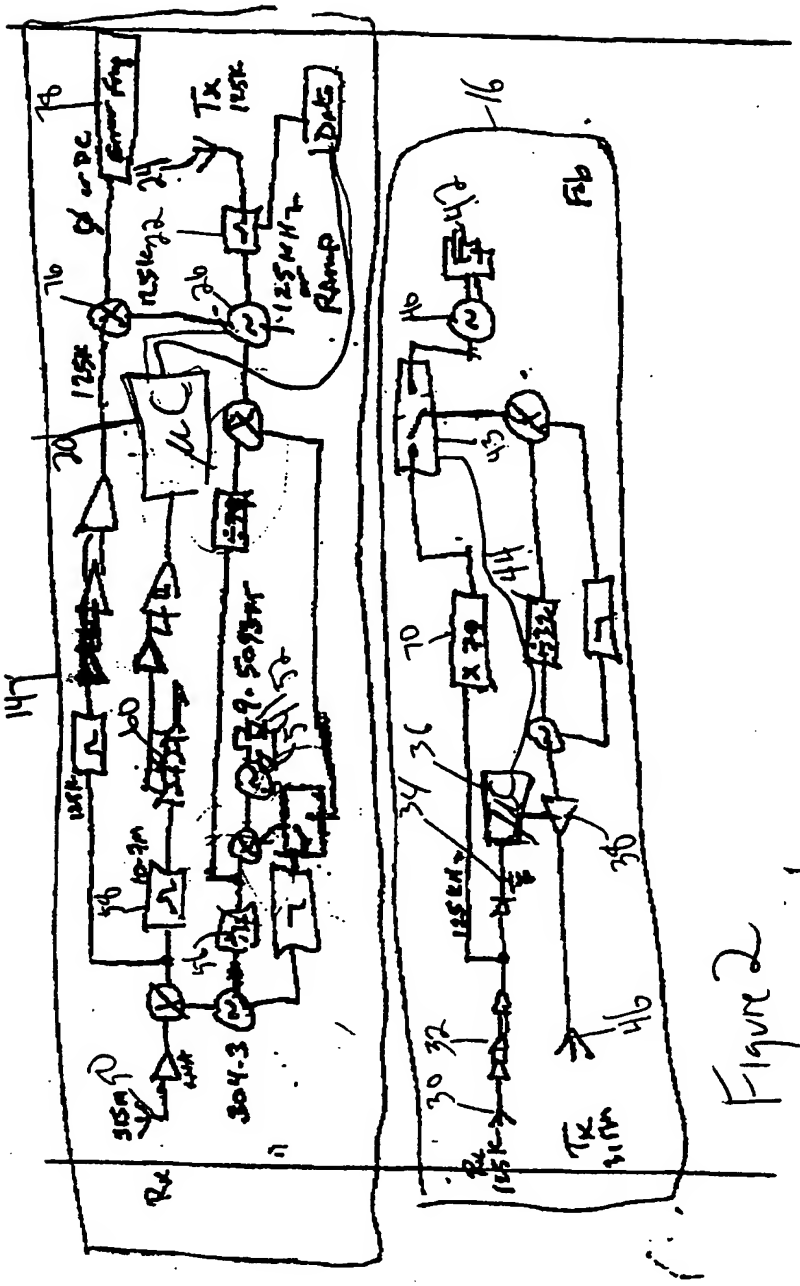

Figure 2

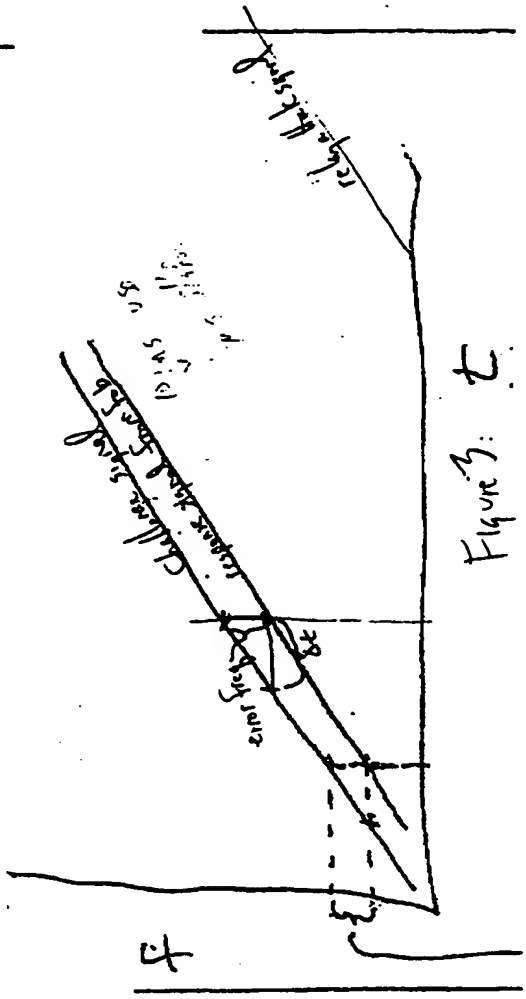

Figure 3